AO 106 (Rev. 04/10) Application for a Search Warrant

EC

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Information, including the content of communications, of the Apple iCloud account associated with Apple ID Lttrucking28@gmail.com, that is stored at premises controlled by Apple, Inc.

Case No. 2:21-mj-603

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

SEE ATTACHMENT A

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 2251, 2252, 2252A	Production, Receipt, Distribution, Possession of Child Pornography
18 U.S.C. 2422(b)	Coercion and Enticement of a Minor to Engage in Prostitution

The application is based on these facts:

SEE ATTACHED AFFIDAVIT INCORPORATED HEREIN BY REFERENCE

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Nate Simon
Applicant's signature

HSI SA Nate Simon
Printed name and title

Sworn to before me and signed in my presence. via facetime

Date: 9/21/2021

Elizabeth A. Preston Deavers
United States Magistrate Judge
Judge's signature

City and state: Columbus, Ohio

Elizabeth A. Preston Deavers, U.S. Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO,
EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF:	)	
	)	**No.**
Information, including content of communications,	)	
associated with Apple iCloud account related to Apple	)	**Magistrate Judge**
ID Lttrucking28@gmail.com that is stored at premises	)	
controlled by Apple, Inc.	)	

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Nate Simon, a Special Agent with Homeland Security Investigations (HSI), being duly sworn, hereby depose and state:

I. EDUCATION, TRAINING, AND EXPERIENCE

1. I have been employed as a Special Agent ("SA") of Homeland Security Investigations ("HSI"), since March 2003, and am currently assigned to the Assistant Special Agent in Charge (ASAC) Columbus, Ohio. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center (FLETC) and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have been assigned to the Franklin County Internet Crimes Against Children (ICAC) Task Force investigating child exploitation offenses since October 2014. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, 2252A, and 2422(b) and I am authorized by law to request a search warrant.

II. PURPOSE OF THE AFFIDAVIT

2. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises owned, maintained, controlled, or operated by Apple Inc. ("Apple"), an electronic communications service and/or remote computing service provider headquartered at One Apple Park Way, Cupertino, California. The property to be

searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

3. The facts set forth below are based upon my own personal observations, investigative reports, and information provided to me by other law enforcement agents. I have not included in this affidavit all information known by me relating to the investigation. I have set forth only the facts believed to be necessary to establish probable cause that violations of 18 U.S.C. §§ 2251, 2252, 2252A, and 2422(b) have been committed by Timothy W. Wright, and that evidence, instrumentalities, contraband, and or fruits of these crimes will be located within the Apple iCloud account that is associated with Apple ID "Lttrucking28@gmail.com" (the **SUBJECT ACCOUNT**). I have not withheld any evidence or information that would negate probable cause.

III. APPLICABLE STATUTES AND DEFINITIONS

4. Title 18 United States Code, Section 2251(a) makes it a federal crime for any person to employ, use, persuade, induce, entice, or coerce any minor to engage in, or have a minor assist any other person to engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct, if such person knows or has reason to know that either the visual depiction will be transported or transmitted via a facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, or that the visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce, or that the visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce. Subsection (e) of this provision further prohibits conspiracies or attempts to engage in such acts.

5. Title 18 United States Code, Section 2251(d)(1)(A) makes it a federal crime for any person to make, print, publish, or cause to be made, printed or published, any notice or advertisement that seeks or offers to receive, exchange, buy, produce, display, distribute or reproduce, any visual depiction involving the use of a minor engaging in sexually explicit conduct, if such person knows or has reason to know that the notice or advertisement will be transported using any means or facility of interstate commerce, or in or affecting interstate or foreign

commerce, including by computer, or if the notice or advertisement has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer.

6. Title 18 United States Code § 2252 makes it a crime to knowingly transport, ship, receive, distribute, sell or possess in interstate commerce any visual depiction involving the use of a minor engaging in sexually explicit conduct.

7. Title 18 United States Code § 2252A(a)(2) makes it a crime to knowingly receive or distribute any child pornography that has been mailed or using any means or facility of interstate commerce.

8. Title 18 United States Code § 2422(b) makes it a federal crime for any person to knowingly use a means or facility of interstate commerce to persuade, induce, entice, or coerce or attempt to persuade, induce, entice or coerce, any individual who has not attained the age of 18 years, to engage in prostitution.

9. As it is used in 18 U.S.C. §§ 2251 and 2252, the term "sexually explicit conduct" is defined in 18 U.S.C. § 2256(2)(A) as actual or simulated: sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or pubic area of any person.

10. As it is used in 18 U.S.C. § 2252A(a)(2), the term "child pornography"[1] is defined in 18 U.S.C. § 2256(8) as: any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where: (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

11. The term "sexually explicit conduct" has the same meaning in § 2252A as in § 2252, except that for the definition of child pornography contained in § 2256(8)(B), "sexually explicit conduct" also has the meaning contained in § 2256(2)(B): (a) graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or

1 The term child pornography is used throughout this affidavit. All references to this term in this affidavit and all Attachments hereto include both visual depictions of minors engaged in sexually explicit conduct

opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited; (b) graphic or lascivious simulated; (i) bestiality; (ii) masturbation; (iii) sadistic or masochistic abuse; or (c) graphic or simulated lascivious exhibition of the genitals or pubic area of any person.

12. The term "minor", as used herein, is defined pursuant to Title 18, United States Code, Section 2256(1) as "any person under the age of eighteen years."

13. The term "graphic," as used in the definition of sexually explicit conduct contained in 18 U.S.C. § 2256(2)(B), is defined pursuant to 18 U.S.C. § 2256(10) to mean "that a viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted."

14. The term "visual depiction," as used herein, is defined pursuant to T18 U.S.C. § 2256(5) to "include undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image."

15. The term "computer"[2] is defined as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. . . " (18 U.S.C. §§ 1030(e)(1) and 2256(6)).

IV. BACKGROUND REGARDING APPLE ID and iCLOUD

16. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

17. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video

---

as referenced in 18 U.S.C. §§ 2251 and 2252 and child pornography as defined in 18 U.S.C. § 2256(8).
2 The term "computer" is used throughout this affidavit to refer not only to traditional laptop and desktop computers, but also to internet-capable devices such as cellular phones and tablets. Where the capabilities of these devices differ from that of a traditional computer, they are discussed separately and distinctly.

calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs enables iCloud to be used to synchronize webpages opened in the Safari web browsers on all of the user's Apple devices. iWorks Apps, a suite of productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

18. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism. An Apple ID takes the form of the full email address submitted by the user to create

the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.

19. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

20. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

21. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an

Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

22. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

23. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

24. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

25. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time.

As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

26. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

27. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

28. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users

V. INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

29. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

VI. INVESTIGATION AND PROBABLE CAUSE

30. In late July of 2021, Special Agents (SAs) from Homeland Security Investigations (HSI) received information from the Delaware County Juvenile Court and Columbus Division of Police Missing Persons Unit (CPD) regarding three minor females. More specifically, SAs learned that

in early to mid-July, a 16-year-old female (herein referred to as MV1), and a 15-year-old female (herein referred to as MV2), and a 17-year-old female (herein referred to as MV3), had all been reported missing. Furthermore, SA's learned that all three MV's were good friends that had gone missing in May 2021, been recovered, and then gone missing again in July 2021. SAs also received information that the MV's were possible victims of sex trafficking.

31. During the investigation into the whereabouts of all three MV's, law enforcement spoke to a family member of MV2 on July 27, 2021. During that conversation, law enforcement learned that MV2 had been receiving multiple phone calls from phone number (352) 302-2819 and had also been dialing that same phone number. To ascertain who MV2 had been communicating with, an open-source search for the phone number (352) 302-2819 was completed. Law enforcement learned from that search that the phone number belonged to a company listed as L&T Trucking and an individual by the name Timothy WRIGHT.

32. On July 28, 2021, investigators also spoke with a family member of MV3 and learned that on May 30, 2021, MV3's family member had received a payment from the Cash App account $Lttrucking28 for the sole purpose of turning MV3's phone back on. More specifically, law enforcement learned that MV3 had contacted her family member from an unidentified phone number to coordinate this payment from the $Lttrucking28 Cash App account. In addition, when MV3 called her family member to set up this payment, law enforcement learned that MV3 was with MV2 and an unknown male's voice was also heard in the background whom MV3 later identified as MV2's "sugar daddy."

33. On July 29, 2021, investigators also learned from a family member of MV1 that MV1 had last been seen leaving the home in a newer black Cadillac Escalade with no front plate being driven by a white unknown male.

34. Investigators conducted an on open-source search in the Cash App application for the profile of $Lttrucking28 which revealed a vanity name listed as Tim Wright (WRIGHT).

35. Investigators conducted records checks with through the Ohio Bureau of Motor Vehicles which revealed WRIGHT had a listed address of 4329 Wyandotte Woods Blvd, in Dublin, Ohio. WRIGHT had registered this Dublin, Ohio address on his most recent driver's license and in addition, WRIGHT used this same address to register a 2021 black Cadillac Escalade bearing Ohio license plate HDZ5952.

36. On July 29, 2021, SAs served a subpoena to Square, Inc. for subscriber information relating to the Cash App account, $Lttrucking28. That same day SAs received the following identifying subscriber information for the $Lttrucking28 Cash App account:

Full name: Timothy WRIGHT

Date of Birth: 08/03/1971

Last four of Social: 8531

Phone Number: (352) 302-2819

37. The phone number (352) 302-2819 received from Cash App is owned by AT&T. On July 29, 2021, SAs served a subpoena to AT&T for subscriber information related to the above-mentioned phone number linked to WRIGHT. That same day SAs received the following identifying information:

Financial Liable Party: L&T Trucking Inc.

Contact Name: Timothy WRIGHT

Contact Home Email: Lttrucking28@gmail.com

38. In addition to the subscriber information received from AT&T, call records were received which indicated the cell phone associated with WRIGHT's (352) 302-2819 phone number was an Apple iPhone X. In review of those call records, SAs noted between May 2021 and July 2021, phone calls and text messages were made between WRIGHT and MV2 as well as WRIGHT and MV3.

39. On July 31, 2021, Franklin County Sheriff's Office (FCSO) obtained a search warrant for WRIGHT's iPhone X bearing serial number G0NW2EV0JCL8 and IMSI number 310410066384069. On August 2, 2021, FCSO located WRIGHT at his Dublin, Ohio residence and the iPhone X was given to officers by WRIGHT upon arrival at the residence pursuant to the search warrant.

40. Law enforcement then engaged in a consensual conversation with WRIGHT at his residence. During that conversation, WRIGHT was shown a photograph of all three MVs. WRIGHT indicated he recognized the face of MV1 but did not know her true name. WRIGHT stated he also recognized MV2 and knew her by a nickname and recognized MV3 whom he knew by true first name. WRIGHT stated that he thought all three MVs were 18 years old and that he had previously tried to "help them out." WRIGHT also admitted that he had all three MVs to his house before and that the last time he had seen them, WRIGHT had picked up MV1 from MV1's house and had dropped all MVs off at an unknown location north of I-71. WRIGHT further indicated that he did not know the current whereabouts of any of the MVs.

41. A cursory review of the iPhone X confirmed that MV2's nickname and real name were one of WRIGHT's contacts listed in the iPhone X. In addition to that, during the cursory review, officers observed images depicting what appeared to be nude female minors.

42. Based on the cursory review, law enforcement obtained a second search warrant for the iPhone X on August 9, 2021.

43. On August 10, 2021, a forensic extraction of the iPhone X was completed. In the initial review of that extraction, law enforcement recovered text messages via iPhone messenger which, in summary, indicated that WRIGHT coordinated dates and times to meet with the MVs, negotiated prices for nude or explicit photographs of all three MVs, and paid MV2 and MV3 via the Cash App application for nude photographs.

44. More specifically, a review of a portion of the text messages from that extraction revealed that WRIGHT and MV3 had been in contact between the dates of June 9, 2021 and July 15, 2021. Law enforcement specifically noted the following two conversations between MV3 and WRIGHT:

- On June 9, 2021, at approximately 5:15pm, MV3 sent a text message to WRIGHT containing images and videos which depicted MV3 wearing a tank top and underwear. In response, WRIGHT sent a text message to MV3 stating "those are nice, but not nude lol… Send some of your front :)" MV3 then sent WRIGHT a five second video depicting her nude genitalia. Text messages further indicate that, at the request of MV3, WRIGHT send the money owed to MV3 for the nude videos to MV2.

- On June 14, 2021, at approximately 4:35pm, text messages reveal that MV3 and WRIGHT were negotiating a price they both could agree on in exchange for MV3 sending WRIGHT nude images of herself. Specifically, MV3 sent WRIGHT a text stating "100 or less?" WRIGHT then responded with "yeah a lot less lol….I'm more into the meetings instead of pics." MV3 then followed up with WRIGHT and sent a text message stating "50?...75?" In response, WRIGHT wrote "how about 40 lol….I only need a few pics/videos". MV3 then agreed with WRIGHT on that price and indicated to WRIGHT that she will send it.

- On June 14, 2021, at approximately 5:14pm. MV3 sent a text message to WRIGHT which contained a six second video depicting MV3 displaying her nude genitalia and face. MV3 then sent WRIGHT a second text message containing another six second video which depicted MV3 using her hand to spread apart her nude genitalia. WRIGHT then responded to both videos "wow!nice (heart eyes emoji)….def can't wait to see it in person 😊".

45. Further review of text messages revealed that on June 9, 2021, WRIGHT negotiated with MV2, indicating to MV2 that he would pay MV2 $60. In exchange for that money, MV3 was to send three nudes that included MV3's face. WRIGHT then noted to MV3 that the portion of the $60 that belonged to MV3 was in exchange for the video that MV3 had sent WRIGHT on June 9,

2021. SAs knew that video to be the five second video of MV3 which depicted MV3's nude genitalia.

46. Law enforcement also recovered a text message exchange occurring on June 9, 2021 in which WRIGHT asked MV3 her age. In response, MV3 stated "17 years old."

47. In continuing the investigation into WRIGHT, SAs then compared the above text messages from WRIGHT's iPhone X with the results from the Cash App subpoena. In that comparison, SAs documented two payments labeled "personal" to MV2 on June 9, 2021, which SAs noted was the same date the text messages indicated WRIGHT was sending money to MV2 via the Cash App. The first payment was in the amount of $60 and the second was in the amount of $30. Both payments were sent to MV2 from the $Lttrucking28 Cash App account.

48. In addition, SA's documented one payment labeled "personal" to MV3 for $40 on June 14, 2021. This was the same date MV3 had sent WRIGHT a video depicting MV3 using her hand to spread apart her nude genitalia. The payment to MV3 was sent from WRIGHT again using the $Lttrucking28 Cash App account.

49. Furthermore, the investigation revealed that the results of the Cash App subpoena return indicated WRIGHT had transferred over $1200 to the three MVs between May 1, 2021, and July 29, 2021.

50. On August 12, 2021, all three MVs were recovered together in the Columbus, Ohio area. On August 18, 2021, an interview of all three MVs were conducted separately at the Child Assessment Center (CAC).

51. During the interview with MV1, MV1 indicated she sent WRIGHT three pictures of herself depicting partial nudity when she was 16 years old, and that in exchange, WRIGHT paid her $60 via Cash App using a trucking company account. MV3 identified herself in a screenshot of a photo she sent WRIGHT which had been recovered off WRIGHT's iPhone X. According to MV1, WRIGHT offered more money for nude pictures of her vagina, but she didn't feel comfortable and never sent them.

52. During the interview with MV2, MV2 indicated she met WRIGHT less than a year ago. MV2 stated she had been to WRIGHT's house and went there with MV1 and MV3. MV2 confirmed that WRIGHT sent MV2 money through CashApp or paid her in cash for nude pictures. MV2 identified herself in a screenshot of a nude video she sent WRIGHT which had been recovered off WRIGHT's iPhone X. MV2 stated that WRIGHT paid as much as $300 - $400 for his encounters with MV2. In addition, MV2 stated that when she arrived at WRIGHT's house, she went upstairs to WRIGHT's bedroom where he masturbated and ejaculated on her

body. MV2 stated that WRIGHT took her shirt off and tried pushing his penis into her vagina but that they never had sex. MV2 confirmed that WRIGHT knew her true age.

53. During the interview with MV3, MV3 stated she went to WRIGHT's house located in Dublin, Ohio at least five times in a five-week period beginning in June or July of 2021. MV3 stated that when she was at his house, she would lay naked on WRIGHT's bed with her legs spread apart. WRIGHT would then masturbate and ejaculate on to her stomach area. In exchange for that sex act, WRIGHT would pay MV3 $300 and MV3 stated she received that money via Cash App or in cash. MV3 also stated she sent WRIGHT nude videos via text message in exchange for money and identified herself in a still image that depicted MV3 and her nude genitalia which had been recovered off WRIGHT's iPhone X.

54. On August 30, 2021, a new federal search warrant for all of the content contained on WRIGHT's iPhone X was obtained and executed.

55. On August 31, 2021, WRIGHT was arrested pursuant to a federal criminal complaint and arrest warrant relating to his child exploitation activities as noted above.

56. On September 1, 2021, a new forensic examination and analysis was completed for WRIGHT's iPhone X. A review of that forensic analysis confirmed that the phone number associated with the device was (352) 302-2819. In addition, your affiant noted that WRIGHT was utilizing the Apple ID "Lttrucking28@gmail.com" (**SUBJECT ACCOUNT**).

57. Review of the forensic analysis of WRIGHT's iPhone X is still ongoing at this time. However, recovered text message conversations between WRIGHT and at least two of the identified victims appear incomplete to your affiant as they abruptly stop and then start again, leaving gaps in time and quick changes in discussed topics. For example, your affiant observed that an iMessage text conversation between MV2 and WRIGHT began on February 16, 2021. Due to their familiarity with one another in this iMessage conversation, it appears that MV2 and WRIGHT had previously spoken, however there is no record of it on WRIGHT's iPhone X. Additionally, it appears images and/or videos associated with messages sent by WRIGHT to the MVS are missing because your affiant is able to observe indicators that those media files exist but cannot see their content. However, based on the information detailed above regarding iCloud services, it is possible that these conversations with the MVs and any attached digital media files that were exchanged during the course of them, were backed up to the iCloud account associated with WRIGHT's Apple ID, the **SUBJECT ACCOUNT**. Your affiant therefore has reason to believe that the content of the Apple account associated with WRIGHT's Apple ID may contain

contraband and evidence of criminal violations of 18 U.S.C. §§ 2251, 2252, 2252A and 2422(b).

VII. CONCLUSION

56. Based on the aforementioned factual information, your affiant respectfully requests that the Court issue a search warrant authorizing the search and seizure of the items described in Attachment A.

57. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

58. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Nate Simon

Nate Simon
Special Agent
Homeland Security Investigations

Sworn to and subscribed before me this 21st day of September 2021.

Elizabeth A. Preston Deavers
United States Magistrate Judge

Elizabeth A. Preston Deavers
United States Magistrate Judge
United States District Court, Southern District of Ohio

ATTACHMENT A
DESCRIPTION OF PROPERTY TO BE SEARCHED

This warrant applies to all information, including content, associated with Apple ID "Lttrucking28@gmail.com" that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cuptertino, CA 95014.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information, to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A. Such information should include the below-described content of the subject accounts from January 1, 2021 to August 2, 2021.

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time

at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWorks (including Pages, Numbers, and Keynote), iCloud Tabs, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), messaging and query logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);

g. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within 10 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes contraband, evidence and/or instrumentalities of violations of 18 U.S.C. §§ 2251(a) and (d), 2252, 2252A, and 2422(b), including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);

b. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

c. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

d. Communications between the subscriber of the account and others regarding the receipt or distribution of child pornography or sexual activity with minors;

e. Any image or video files depicting minors engaged in sexually explicit conduct;

f. Any image or video files depicting clothed minors for comparison to any files depicting minors engaged in sexually explicit conduct;

g. Any correspondence or communications related to any postings on online classified ad websites;

h. Evidence indicating the subscriber's state of mind as it relates to the crimes under investigation; and

i. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.